Please replace the paragraph beginning at page 2, line 5 with the following rewritten paragraph:

B2

--In accordance with one aspect of the invention there is provided a method of operating an authenticating server system for authenticating users at client terminals connected via a data communications network, to control access to a document stored on a resource server, said method comprising performing the following steps in said server system:

storing authentication details of authorized users:--

Page 3, before line 9, insert as a separate paragraph:

--BRIEF SUMMARY OF THE DRAWINGS--.

Page 4, before line 1, insert as a separate paragraph:

B3

--DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS OF THE INVENTION--.

Please replace the paragraph beginning at page 4, line 28 with the following rewritten paragraph:

B4

--The SPS has an associated data store 8 which holds authentication details for each of the users authorized to have access to the application servers APS and a token identifying the access rights of each user. The CMS has an associated data store 10, which holds details of users currently logged on for

B4 access to the application server APS, and which maintains logging on histories for users once they are logged off.--

Please replace the paragraph beginning at page 8, line 3 with the following rewritten paragraph:

--At this point, the user is fully logged-on in a CMS, with the log on notification details stored in the CMS store 10. B5 The user may then, via an appropriate application client APC access one or more of the application servers APS which the user is authorized to access, as specified by the access right token.--

Please replace the paragraph beginning at page 10, line 25 with the following rewritten paragraph:

--The authentication scheme described in relation to users at terminals T1 or T2 described above involves identification of a user, after initial authentication, by the IP address of the terminal at which the user is logged on. Because the CMS performs periodic re-authentication of the user, it is difficult B6 for a third party to impersonate the user by IP address spoofing. Namely, even if a third party were to spoof the IP address of the user, the third party would only have access to the real user's resources for the time provided by the user's timer in the CMS. Once the timer has expired, the third party forming the IP spoofing would not be able to re-authenticate, without access to the user's password. Since the user's password is only ever sent across the Internet when a

B6

password change occurs, and even then in encrypted form, a third party has no means of finding out the password of an authorized user.

Please replace the paragraph beginning at page 12, line 24 with the following rewritten paragraph:

B7

--In return, the APS receives the authentication details from the APC, step 84, including the same address token, whereby the user is re-identified, and the username and password, on which the SPC performs the first hashing function H0 illustrated in Figure 4. This information is passed on to the CMS, which polls the SPS to check whether the username and password hash matches one stored in the SPS store 8 as that of an authorized user.--

Please replace the paragraph beginning at page 17, line 31 with the following rewritten paragraph:

B8

--Each data block includes five parts, including an initialization vector 150 for the decryption process, added during encryption and prior to transmission of the block. The block also includes a block number, 152, which increments with each block of data sent, and a data count 154, which is a count of the number of data bytes included in the data block, excluding the initialization vector 150, block number, data count, checksum and any padding added during the encryption process. The next part of the data block is the part holding the encrypted data 156, which is padded to a multiple of 8 bytes by the encryption function if the data block is not otherwise a multiple of 8 bytes. The